CLAIMS

What is claimed is:

1. A method for providing access protection to electronic storage devices, said method comprising the steps of:

providing a hardware-level security code for a storage device on which is stored an electronic file to which restricted access is desired; and

allowing access to said storage device only when a user enters a user code that matches said security code.

2. The method of Claim 1, further comprising the steps of initializing said security code within a microcode of said storage device, wherein access to said storage device is denied during said initializing step.

3. The method of Claim 1, further comprising the step of defining an operating system (OS) extension and corresponding OS extension process by which said allowing step is implemented.

4. The method of Claim 3, wherein said defining step includes:

adding a hardware security code checking process to an OS operation for supporting a security code comparison with a user access code when a user requests a read and write on said storage device.

5. The method of Claim 4, further comprising the step of:

evaluating via said hardware security code checking process said security code returned by said file protocol; and

in response to said security code having a pre-determined default value, providing said user with unrestricted access to said storage device.

6. The method of Claim 5, further comprising the step of comparing said security code with said user provided access code when said authentication code is not said pre-determined default value.

7. The method of Claim 5, further comprising the step of outputting an access deny message of said user.

8. The method of Claim 7, further comprising the steps of:

restricting a subsequent request for access to said storage device by a user when said security code does not match said user access code during an initial request by said user; and

terminating a job submitted by said user.

9. A computer program product comprising:

a computer readable medium; and

program instructions stored on said computer readable medium for implementing file access protection by:

providing a security code for a drive on which is stored an electronic file to which restricted access is desired; and

allowing access to said drive only when a user access code that matches said security code is provided.

10. The computer program product of Claim 9, further comprising program instructions for initializing said security code within a microcode of said drive, wherein access to said drive is denied during said initializing step.

11. The computer program product of Claim 9, further comprising program instructions for implementing an operating system (OS) extension.

12. The computer program product of Claim 11, further comprising program instructions for:

adding a hardware security code checking process to an OS operation for supporting a security code comparison with a user access code when a user requests a read and write with respect to said storage device.

13. The computer program product of Claim 12, further comprising program instructions for:

evaluating via said hardware security code checking process said security code returned by said file protocol; and

in response to said security code having a pre-determined default value, providing said user with unrestricted access to said storage device.

14. The computer program product of Claim 13, further comprising program instructions for comparing said security code with said user code when said security code is not said pre-determined default value.

15. The computer program product of Claim 13, further comprising program instructions for outputting an access denied message of said user, and canceling the job submitted by said user.

16. The computer program product of Claim 15, further comprising program instructions for restricting a subsequent request for access to said storage device by a user when said security code does not match said user access code during an initial request by said user.

17. A data processing system comprising:

a processor;

a memory linked to said processor via an interconnect;

an input/output (I/O) device;

a drive on which is stored one or more files for which restricted access is desired; and

an OS executing on said processor that provides support for assigning a hardware-level security code for said drive and allows access to said file by user only when a user entered access code matches said security code.

18. The data process system of Claim 17, wherein further said OS includes an OS extension by which an assigning of said security code and access to said drive are implemented.

19. The data process system of Claim 18, wherein further said OS extension includes program instructions for:

adding a hardware security code checking code to an OS operation for supporting a security code comparison with a user access code when a user requests a read and write on said drive; and

identifying specific locations on flash ROM or EEPROM that houses drive microcode on said drive for initializing said security code.

20. The data process system of Claim 18, wherein further said OS extension includes program instructions for:

evaluating via said hardware security code checking process said security code returned by said file protocol; and

in response to said security code having a pre-determined default value, providing said user with unrestricted access to said drive.

21. The data process system of Claim 20, wherein further said OS extension processes includes program instructions for comparing said authentication code with said user entered access code when said authentication code is not said pre-determined default value.

22. The data process system of Claim 21, wherein further said OS extension further includes program instructions for outputting an access deny message to said user when said security code does not match said access code.

23. The data processing system of Claim 21, further comprising means for restricting a subsequent request for access to said storage device by a user when said security code does not match said user access code during an initial request by said user.

24. A storage system comprising:

a recordable medium for recording data; and

a security code that is unique to said storage system and which protects said data recorded on said recordable medium from unauthorized access.

25. The storage system of Claim 24, further comprising:

an input/output mechanism; and

means for issuing said security code to a requesting operating system extension.

26. The storage system of Claim 25, wherein said input/output mechanisms connects said storage system with a data accessing device.

27. The storage system of Claim 26, wherein said data accessing device is a processor on which said requesting operating system process executes.